Defense Information Infrastructure Common Operating Environment

(DII COE)

The Way Ahead

Julie A. Surer
DII AF COE Chief Engineer
781-377-6809
jsurer@mitre.org

What is the DII COE

- The DII COE concept can be described as
  - a reference implementation of the DOD Joint Technical Architecture containing a collection of reusable software components
  - a software infrastructure for supporting mission applications and their reuse across Service domains
  - an approach for facilitating integration and enabling interoperability
  - a set of guidelines, standards, and specifications

- GCCS is a C4I System built on top of the DII COE
- GCSS is a collection of Combat Support Systems built on top of the DII COE

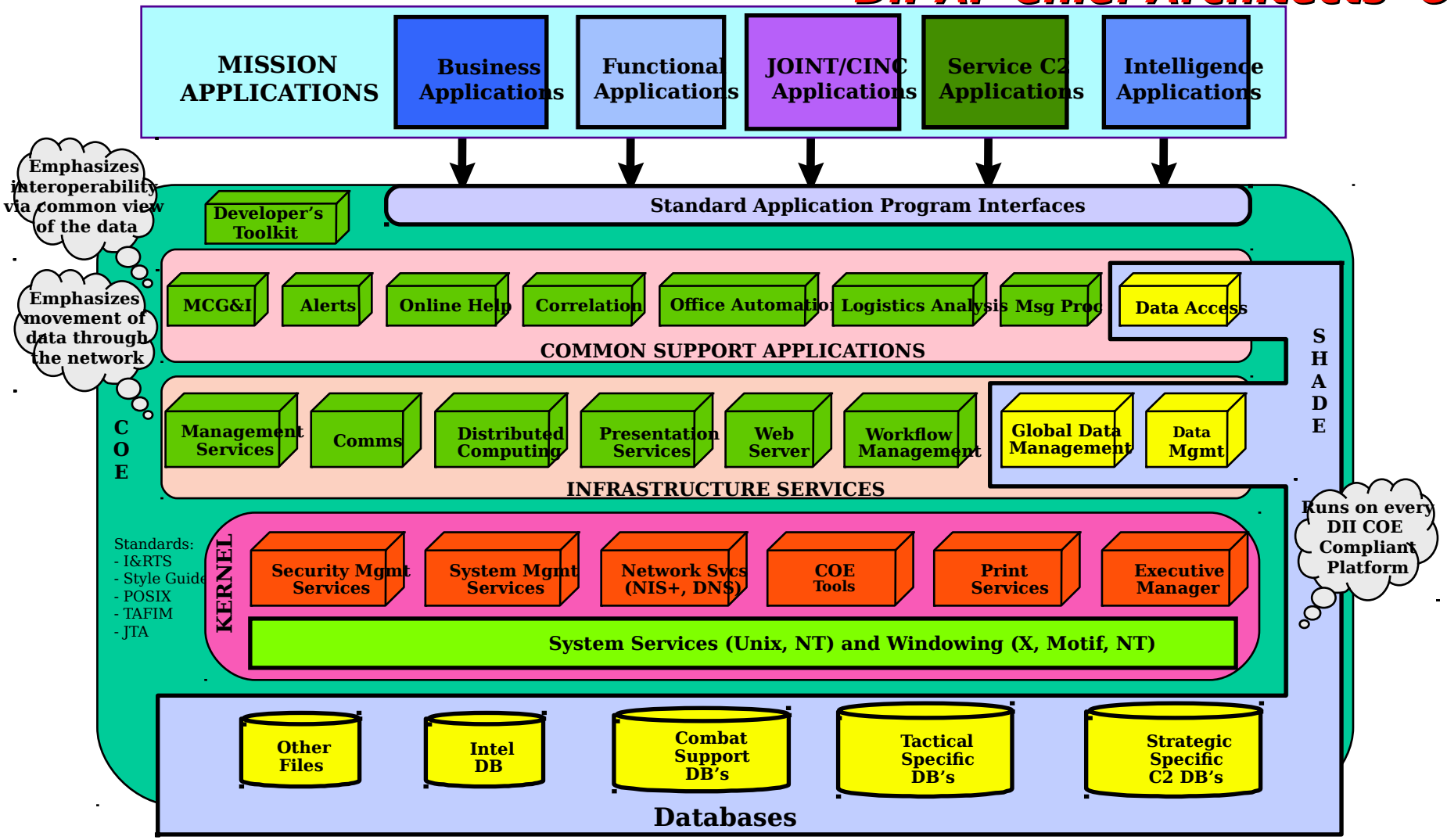
"The DII COE is ***not*** a system; it is a ***foundation*** for building a shared system."

DII COE Principles

- DII COE is an approach for reuse
  - COE components
  - But the mission applications as well
- DII COE helps provide interoperability
  - Implementing standards-based components
  - Defining standard APIs defined
  - Providing standard integration/runtime environment
- Shared Data Environment (SHADE) is as important as runtime
  - Access to and sharing of common data between applications
  - Separation of data and application which creates and/or uses the data
  - Standardized tools for DB distribution and installation

DII COE Taxonomy

DII-AF Chief Architects' Of



DII COE Process

Management Structure

DII-AF Chief Architects' Of

Chair: S/A Lead
Members: S/A Technical Reps
Charter: Requirements, Design, Products (ECP/SCP)

AF leads Distributed Comp., Admin Svc, Office Automation Multimedia, NT Advisory Grp, and Real Time. AF has technical representatives to other TWGs

Key AF Activities:
- Advocate for AF Rqmts
- Offer AF contributions

Chair: DII COE Chief Engr
Cmdr. Ken Wheeler
Members: S/A O-6 & Chief Engr
Charter: Planning, Schedule & Approval, S/A Top Priorities

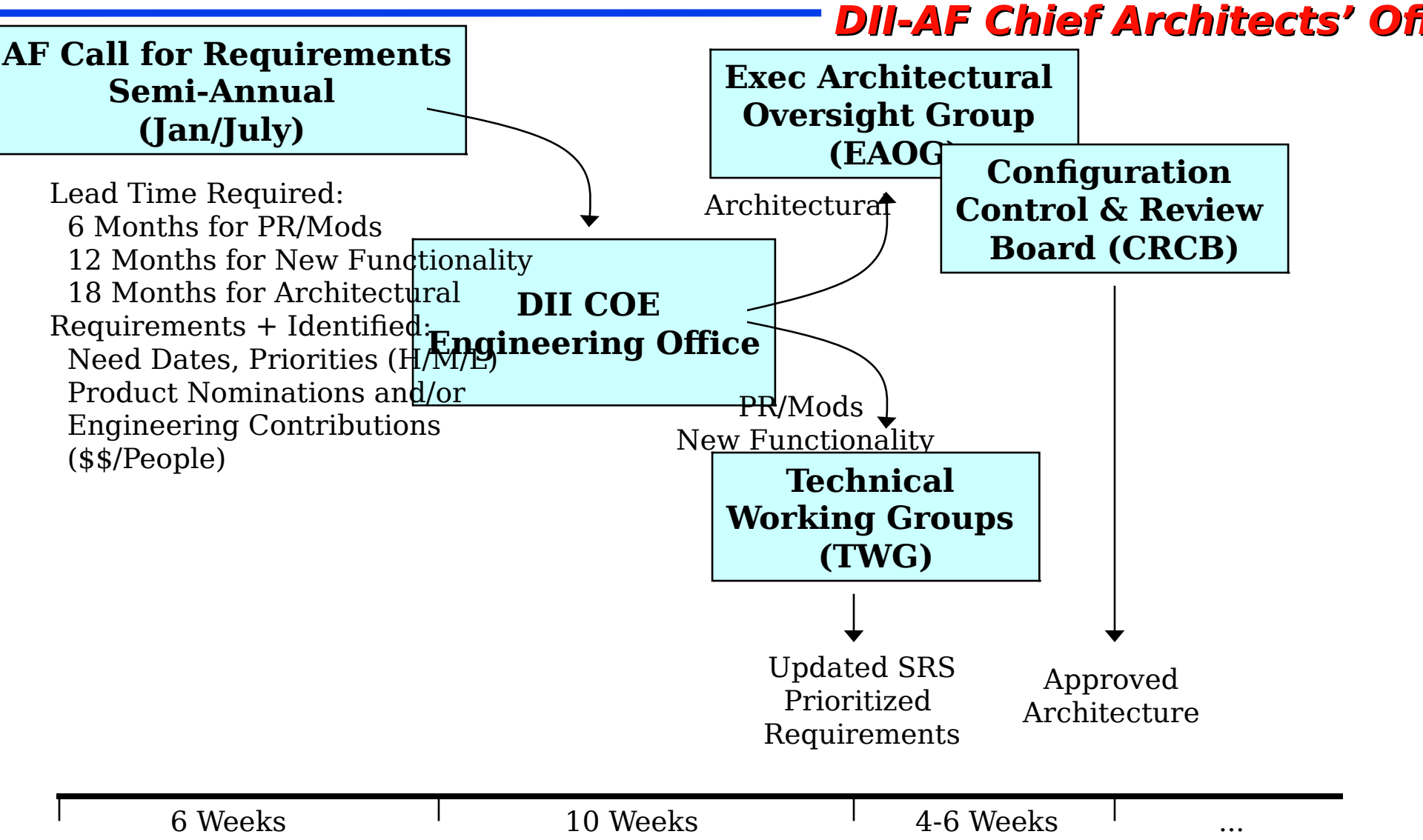
Key AF Activities:
- Review/Approve Build Plan
- DII COE Schedules
- Satisfy AF Priority Rqmts
- Advocate AF Position

Chair: BGen Salisbury
Members: S/A Flag, PEO & Chief Architects
Charter: Final Approval, S/A Commitment, Resources

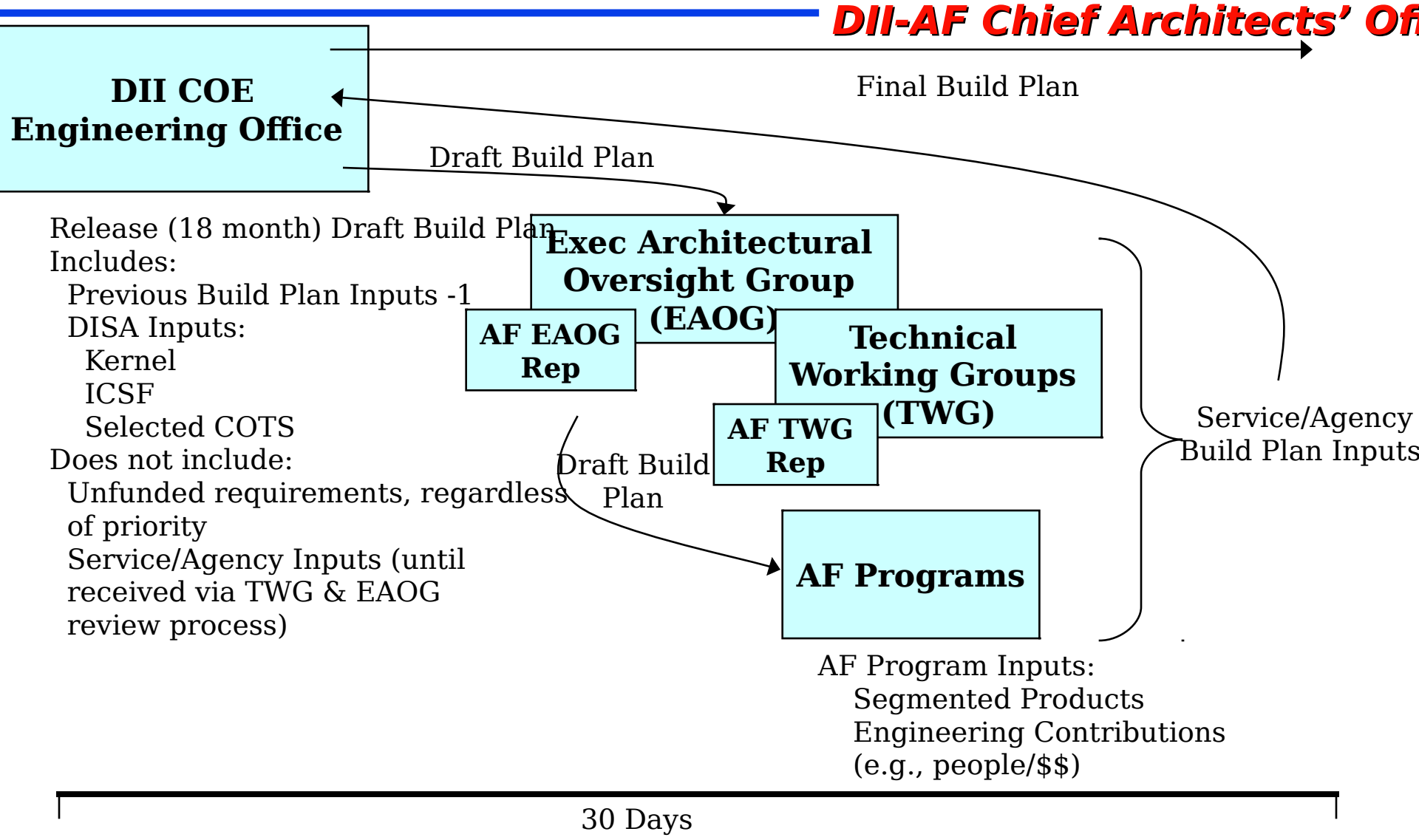
Key AF Activities:
- Approve Build Plan
- Overall DII COE objectives & milestones
- API retirements
- COE directions
- Hardware & Software baseline

Definition and Design ..... Planning and Building .....

Requirements Process



Build Process

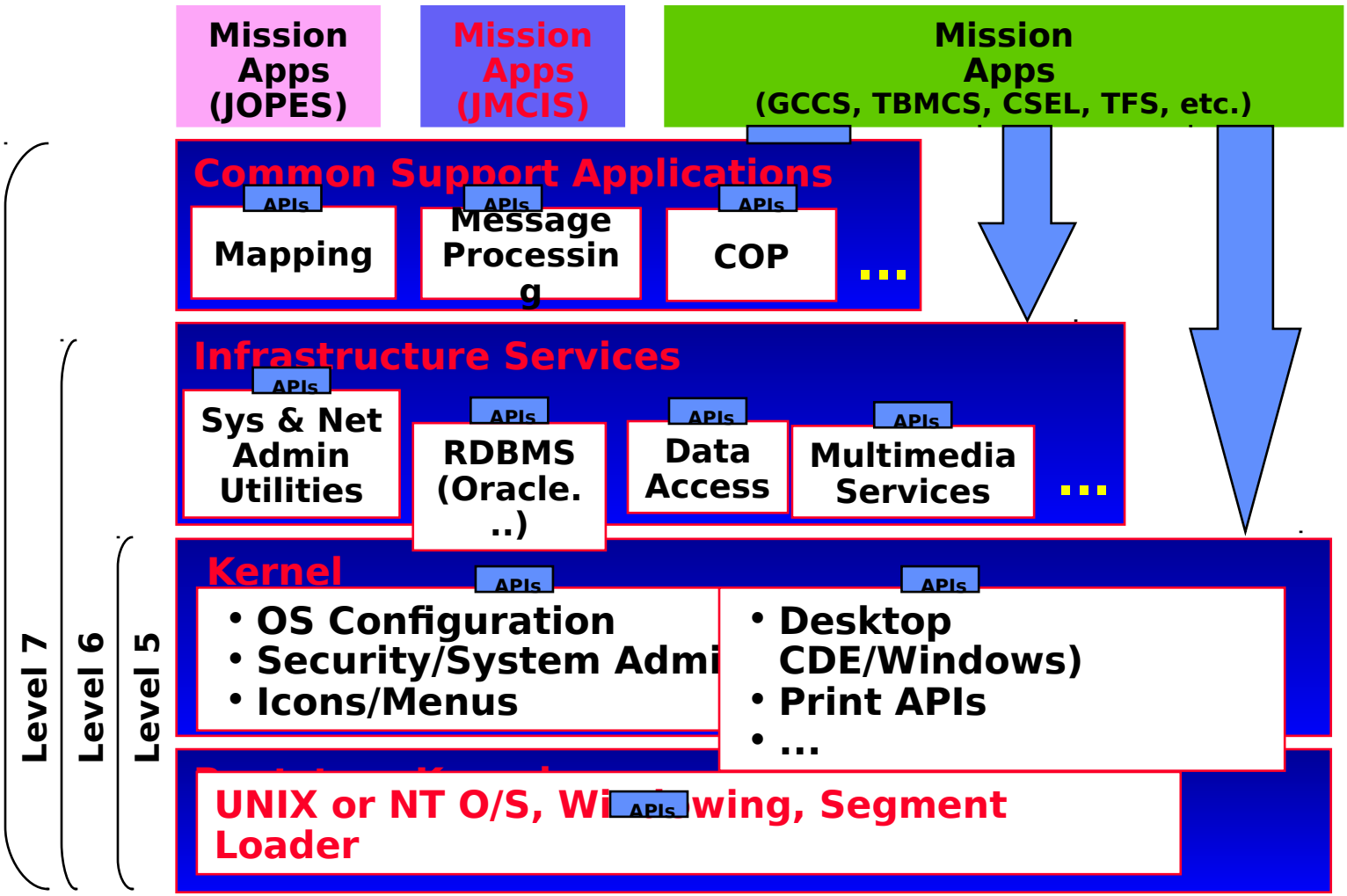


DII COE Compliance

Compliance

- Measures the degree to which your software component can plug-and-play in the COE
- There are four areas of compliance
  - Run Time Environment
  - Style Guide
  - Architectural Compatibility
  - Software Quality
- RunTime Environment (Level 1-8)
  - Determines whether the software is in compliance with the Integration and Run Time Specification (I&RTS)
  - A combination of I&RTS Checklist and COE Compliance Testing Tools are used to determine the level of compliance
  - Waivers are required for deviations

Migration to the COE
Multiple Levels of Integration



DoD Guidance & Mandates

- 23 May 1997 Memorandum from Assistant Secretary of Defense Emmett Paige
  - All UNIX-based C4I legacy systems, other than mainframe based systems, shall be Level 5 DII COE compliant
  - All new C4I emerging systems and upgrades shall be Level 6 DII COE compliant with the goal of achieving Level 7.
- The JTA v2.0 mandates the use of the DII COE
  - … all C4I systems shall use the DII COE. All applications of a system which must be integrated into the DII shall be at least level 5 compliant with a goal of achieving level 8.
- Defense Planning Guide, 1997-2000
  - The foundation for JV2010 is information superiority, of which migration to the DII COE is a key, to include intelligence and logistics systems.

AF Guidance & Mandates

- **LtGen Kadish has directed ESC Programs to be DII COE Level 5 Compliant by Year 2000 … *be prepared for a change*, as ESC may raise the compliance bar (perhaps in line with DoD mandate)**

- **LtGen Muellner, Migration of AF Functionality to DII COE (August 1996) … Migration to the DII COE must occur as rapidly as possible within fiscal constraints. The initial target for integration of these functionalities will be a minimum of Level 5 compliance with an evolution strategy toward higher levels of integration.**

- **AF Planning and Programming Guidance (APPG)**
  - **" All AF developed C2 systems should be on a clear migration path to the DII COE, and new applications must be developed to be COE-compliant when they are initially delivered. "**
  - **This guidance leads to POM direction**

Raising the Bar for AF Level 6 Compliance

- Today, Level 5 by 2000 ... provides a minimum essential compliance that ensures applications are segmented, installable using the COE installation tools, operate with the COE kernel, and can federate on a platform
- Level 6/7 provide additional interoperability and economy by using COE services to integrate information, and by requiring that legacy applications do not duplicate the functionality provided by the COE
- Recommending Level 6 compliance by 2002, but also
  - Targeting a specific version of the DII COE for AF deployment
  - Providing guidance to developers that will make transition from Level 6 to Level 7 compliance easier
- What does it mean to AF programs
  - Incorporating additional COE services, into the system...target COTS and mature GOTS products in the infrastructure layer
  - Contributions of AF COE components
  - Enhanced interoperability ??? ... may need to wait for GNIE

Global Networked Information Enterprise (GNIE)

- ASD (C³I) directed
  - Effort to last 26 months (started in Nov '98)
  - Thrust Areas/Panels include Computing and Communications (Networking, Enterprise Computing, and Interoperability and COE Panels) and Enterprise Management (Network Operations, Information Assurance, and Information Dissemination Management (IDM) Panels)
- COE/Interoperabilty Panel addresses DII COE
  - Developing guidance/policy on interoperability, e.g., joining rules (technical rules for enterprise interoperability at a "least common denominator" level)
  - No impact expected until 2001

An information enterprise that delivers secure, assured, efficient, effect interoperable information services, responsibly, on a global basis -- enabling successful mission accomplishment in support of the warfighter and agencies that provide national security.

GNIE Interoperability/COE Panel Preliminary Thinking...

DII-AF Chief Architects' Of

- **Participation in the enterprise will require...**
  - **For secure operations ...Mandate enterprise security services, e.g., PKI, virus detection**
  - **For minimal enterprise interoperability ...Mandate (where applicable) the use of enterprise infrastructure services, e.g., directory, web, email**
- **Evolve current DII COE kernel and infrastructure services to include implementations of enterprise operating environment services, e.g., PKI, directory services**
- **Continue to mandate and evolve the DII COE for the C4ISR Community of Interest (COI), e.g., C4ISR COE COI**
- **Encourage C4I COE implementation (and process) to other COIs**

GNIE Impact ???

- Contrary to recent press, don't expect the COE to go away
  - The COE has provided the DoD with a "good neighbor policy" for our mission applications so that they can coexist... this is a vast improvement from the stovepipes we used to build
  - DISA, as well as the other Services/Agencies, are improving the COE (e.g., security, robustness, backward compatibility) and evolving the capabilities (e.g., collaborative tools, real time, framework-based)
- The COE concept has been proven ...now we need to address the the *enterprise*...this will evolve COE as we know it today, perhaps as follows
  - Enterprise Operating Environment
    - Based on DII COE kernel with additional security services
    - Based on DII COE Infrastructure Services with additional enterprise services such as directory services
  - Common support applications developed around a specific COI
  - Shared data via standardized approaches, e.g., web, ftp
- Final impact ...stay tuned

DII COE v4.x Series

DII COE v4.x Series

- **DII COE v4.0 (April '99)**
  - **April '99 release is only 8 months away from the millennium, fielding systems on v4.0 becomes prohibitive because of Y2K testing**
  - **As a result, COE 4.0 is being released as a "developer's release" or "beta release"**
  - **Services/Agencies will have more time to get *up to speed* on the COE and provide DISA with problem reports in order to help stabilize v4.1 (October '99)**
- **Re-organized existing software around three-tier principles**
- **Create architecture-independent user interface**
- **Introduce strong security model across (data, application and navigation) layers**

Kernel Overview

- Newly developed Java-based kernel
  - Only published APIs will be honored
  - Java and C APIs will be supported
- Modified kernel architecture with functional enhancements that improve performance and provide greater flexibility in configuring/deploying COE-based systems
  - Enhancements will require changes to how developers build *future* segments, and how integrators and site admins configure the system
  - 3.x segments will be supported in the 4.x
- Stay tuned for details at DII COE Developers Conf (13-15 April)

Kernel Details

- ***Account and Profile Management*** **(APM) provides the "Volkswagen approach" to account management by providing a common look and feel GUI across all COE supported hardware**
- ***Common Data Store*** **(CDS) is a cross-platform data store used by the kernel to store and retrieve data objects and associated attributes (e.g., segment, user and host data)**
- ***Service*****s identify functionality provided by segments and used by services provided by other segments. Services will enable migration to an object oriented distributed network-based architecture**
- ***Features*** **provides the ability for the site administrator to group icons/menus for sets of users**
- ***Bindings*** **will provide the mechanism for fine tuning access control of COE services**

Security Initiatives

DII-AF Chief Architects' Of

- **Identify and Fix DII COE Vulnerabilities**
  - **Operate DII COE IAVA Implementation Process**
  - **Develop/Test/Segment/Release Security Patches**
  - **Conduct DII COE Security Assessments**
- **Integrate Security into COE Design Process**
  - **Develop Security Services Architectures for the COE (e.g. authentication, confidentiality, data integrity, etc.)**
  - **Investigate/Evaluate new or advanced software security technologies**
- **Support DII COE Implementation in the Intelligence Community**
  - **Provide technical guidance to DIA, DODIIS, NSA, NIMA, NRO, & CIA on COE implementation**

AF Initiatives in the COE (Highlights)

Multimedia/Collaborative Services

- **Common Operational Modeling, Planning and Simulation Strategy (COMPASS)**
  - **GCCS v3.0 (Stage II) mission application**
  - **Developed by the Navy and is designed to allow dispersed C2 system users to share tactical information.**
  - **A combination of GOTS, public domain and COTS software**
- **Collaborative Tool Kit (CTK)**
  - **Plug-n-play framework (e.g., common API and user interface for access to the collaborative toolset) and collaboration toolset**
  - **Based on the DARPA/DISA JPO/JDISS efforts**
  - **Similar toolset as COMPASS, e.g., VIC/VAT, although under a different infrastructure**
- **InfoWorkSpace (IWS)**
  - **Potential COE nomination by AF (via TBMCS/EFX)**
  - **Provides collaborative meeting environment via Netscape/IE browser**
  - **Issues: Compatibility with CTK framework; Unbundle 3rd party COTS**

Message Processing

- Common Message Process (CMP) is the standard product for message processing in the COE
  - Army CHS is developer
  - Provides the "Volkswagen Approach" to message processing

- AF (for TBMCS) nominated IRIS Message Formatting System (MFS)
  - COTS message processing capability
  - Adheres to COE architecture by providing, the parser, the interactive USMTF format generator, the automated message generation ...plus other capabilities
  - IRIS Vendor (Systematic) has pledged support of the three COE APIs (mtfval, mtfextract, mdlmap)
  - Segments to be delivered in mid-March

NT Advisory Group

DII-AF Chief Architects' Of

- Development/Segmentation guidance for NT-based systems
  - Develop applications IAW best commercial practices
  - Supplements to *I&RTS* and *How to Segment Guide*
  - Resolves conflicting requirements in *I&RTS*
- New (COTS) segment installer capability expected in v4.0
  - Based on InstallShield w/ COE template
  - Implies abbreviated segmentation for COTS/GOTS
- NT v4.0 Service Pack 4 (SP4) under evaluation
  - SP4 must be installed before Y2K for compliance
  - Issues: SP4 is a major OS upgrade ...may not be compatible w/ existing applications and uninstalling SP4 is not completely reversible
- Impact/Transition to Windows 2000
  - Participate in Microsoft developer forums
  - Articulate AF requirements/issues/concerns

Distributed Computing

DII-AF Chief Architects' Of

- **Distributed Computing Road Map ...expects**
  - **CORBA 2 now thru end 2000; CORBA 3 late 1999 beyond 2002**
  - **COM-CORBA bridges early 1999 thru at least 2000**
  - **Real Time CORBA late 1999 thru 2002 (in support of RT TWG/IPT)**
    - **Segmentation of RT CORBA product, HARDPACK**
    - **Developing RT CORBA validation suite**
  - **CORBA Security early 1999 beyond 2001 (in support of SSTWG)**

- **COM/DCOM/CORBA Interoperability**
  - **White Paper on COM-CORBA interoperation for COE developers**
    - **Usage scenarios which provide description of requirements (GCCS/TBMCS)**
    - **Basic Bridge Approaches & Services**
    - **Performance**
    - **Software processes**
    - **Product recommendations**
  - **C2STA requires COM or CORBA (w/IDL defined interfaces)**

Real Time

- Real Time capabilities are targeted for DII COE v5.0 (Oct '00)
  - A configurable DII COE RT Kernel for LynxOS and Sun Solaris
  - CORBA product with extensions for real-time
  - Support tools for developing RT segments and building customized configurations for real-time
- Systems targeted for DII COE RT include AF Multipurpose C2 Center, Army First Digitized Division, and Navy Common Command & Decision System
- Agreements to date
  - Domain definition
  - Kernel requirements, including
    - Build time integration model
    - Selectable (POSIX Conformant) kernel services
    - Kernel configuration process
    - Build time developer toolkit
- Working funding issue/priorities with DISA
- Briefing to CRCB for Service/Agency flag concurrence

DII COE Futures
v5.x Series

DII COE v5.x Series

- Support for Real Time
- Component framework implementation of services
- Commercialization of (most of) the kernel
- Improved security implementations
- Issues
  - Difficult to predict technology to implement
  - Evolution of JTA

Recent Activities

Systems Engineering IPT

DII-AF Chief Architects' Of

- **DISA formed Systems Engineering IPT to address interoperability issues between major COE-based programs (TMBCS, GCCS, GCCS-M, AGCCS) .**
- **Provides a collaborative forum (and process) for addressing COE-based implementation and system engineering issues associated with how services implement the COE to achieve "plug and play" interoperability, maximum reuse of COE and COE-based mission applications, and synchronization of baselines**
- **Hot Topics**
  - **Flexibility of kernel/security architecture**
  - **Enterprise management**
  - **Common criteria for security accreditation**
  - **Harmonize disparate alerts capabilities**
- **Working directly with DISA on TBMCS kernel dependencies to ensure sufficient flexibility to support web-based architecture**

SCI Accreditation

- DoDIIS will certify DII COE 3.4 with selected COE COTS products for TS/SCI (expected Summer 1999)
  - Tivoli, Axent, McAfee and shareware (e.g., Crack, TCP Wrappers, etc)
  - Several segments from DoDIIS CSE-SS will be used until acceptable COTS becomes available
- DoDIIS CSE-SS will be funded for maintenance only, until June 2001 when discontinued
- DII COE v3.4 kernel patch (to fix security PR's) delivered 1 February (under DoDIIS evaluation)
- DoDIIS to share Security Accreditation documentation and COE configuration information w/ other systems that requirement SCI accreditation (e.g., ESC/IY programs and SCI TBMCS)

CAO Position Papers

DII-AF Chief Architects' Of

- CAO-001 System Administration ... endorses the Tivoli Management Environment for system administra

REVISED

- CAO-002 Win95/98 ...provides guidance on the deployment and migration of Win95/98-based workstations. Also guidance on Win '95 u to Win 98

FINAL

- CAO-004 Network-based Clients ...defines standards for DII COE compliant Network-based clients

FINAL

- CAO-005 NT Interim Guidance ..provides supplemental development guidance for NT-based systems

FINAL

- CAO-008 NT Segmentation ...provides guidance on partial segmentation for NT-based software due to conflict in the current version of the Integration and Run Time Specification

DRAFT

Closing Remarks

DII-AF Chief Architects' Of

- **Interoperability needs *will* continuously change and evolve ...therefore, *flexibility* is key to sharing information across the enterprise**
- **The Integrated C2 System (IC2S) is an effort to realize the AF vision of an integrated set of C2 (combat ops, combat support and business systems) capabilities**
  - **IC2S Program Office Cadre will orchestrate acquisition efforts across ESC in order to achieve the delivery of an integrated capability**
  - **Domain engineering efforts will identify and resolve duplication of AF mission capabilities**
  - **To ensure *flexibility* is built in...**
  - **The C2 System Target Architecture (C2STA) sets forth the *how to's* for realizing and building an integrated capability**
  - **The DII COE (and JTA) provides the common infrastructure to facilitate integration, interoperability and reuse**